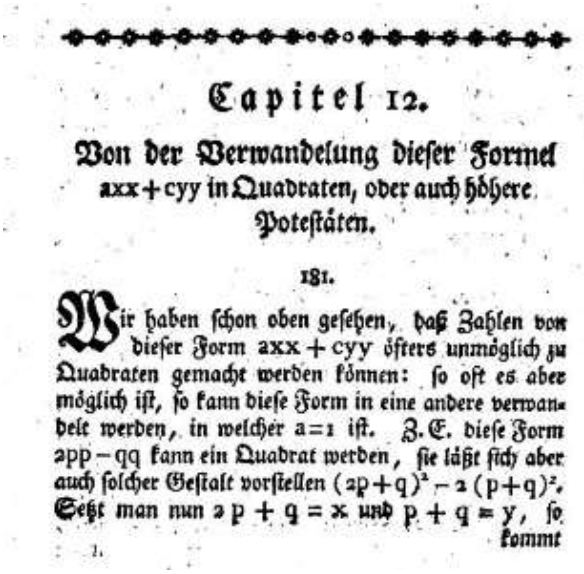
Euler on the case $n = 3$ of Fermat's Last Theorem

A proof, based on the infinite descent method, is contained in the textbook *Vollständige Anleitung zur Algebra* (St. Petersburg, 1770). It appears in Section, Chapter 12, under a title which can be translated as *On the transformation of this formula axx+cyy in squares, or also higher powers.*



Capitel 12.

Von der Verwandelung dieſer Formel axx+cyy in Quadraten, oder auch höhere Poteſtäten.

181.

Wir haben ſchon oben geſehen, daß Zahlen von dieſer Form axx + cyy öfters unmöglich zu Quadraten gemacht werden können: ſo oft es aber möglich iſt, ſo kann dieſe Form in eine andere verwandelt werden, in welcher a=1 iſt. Z. E. dieſe Form 2pp − qq kann ein Quadrat werden, ſie läßt ſich aber auch ſolcher Geſtalt vorſtellen $(2p+q)^2 - 2(p+q)^2$. Setzt man nun $2p + q = x$ und $p + q = y$, ſo kommt

The argumentation can be sketched as follows. Suppose for a contradiction that $x^3 + y^3 = z^3$ for some nonzero integers x, y, z. Without loss of generality we may assume that x, y are coprime. Then two of the three numbers are odd, and one is even. Up to moving terms from one side to the other, we further may assume that x, y are odd. If we wish to restrict ourselves to the case where x, y are both positive, we will have to consider the equation $x^3 - y^3 = z^3$ as well. This, however, as it will turn out in a moment, does not require a separate proof. Suppose that $x > y$. Let p, q be positive integers such that $x = p + q,\ y = p - q$. Then p, q are coprime, and we get

$$x^3 + y^3 = 2p\left(p^2 + 3q^2\right)$$
$$x^3 - y^3 = 2q\left(q^2 + 3p^2\right)$$

Thus it suffices to show that a number of the form $2p\left(p^2 + 3q^2\right)$ is never a (perfect) cube. We may assume that p is even, so that q is odd (otherwise p and q would be exchanged, y would be replaced by $-y$ and we would turn to the second equality). Once again, suppose for a contradiction that $2p\left(p^2 + 3q^2\right)$ be a cube. Since p is even and the second factor is odd, it follows that p is divisible by 4. Moreover the product of integers $\frac{p}{4}\left(p^2 + 3q^2\right)$ is a cube, too. We will only consider the case where the two factors are coprime. If they are not, the coprimality of p, q implies that their only positive non trivial common divisor is 3, so that $3|p$ and $3\nmid q$. If $p = 3r$, then we get, as a new cube, the product of coprime integers $\frac{9r}{4}\left(3r^2 + q^2\right)$, which can be handled in a similar way. Note that both factors $\frac{p}{4}$ and $p^2 + 3q^2$ are cubes. At this point, Euler claims the existence of two integers s, t such that

$$\begin{aligned} p + q\sqrt{-3} &= \left(s + t\sqrt{-3}\right)^3 \\ p - q\sqrt{-3} &= \left(s - t\sqrt{-3}\right)^3, \end{aligned} \tag{1}$$

whence $p^2 - 3q^2 = \left(s^2 + 3t^2\right)^3$, and, moreover,

$$2p = 2s(s+3t)(s-3t)$$
$$q = 3t(s+t)(s-t)$$

Recall that $2p$ is a cube, and that p, q are coprime, which implies that so are s, t, and that $3 \nmid s$. On the other hand, since q is odd, t is odd and s is even. It follows that $2s,\ s+3t,\ s-3t$ are pairwise coprime, hence each of them is a cube. Let u, v be integers such that $s+3t = f^3,\ s-3t = g^3$. Then the sum $f^3 + g^3 = 2s$ is a cube, say h^3. We have just found a new solution (f, g, h) to Fermat's equation, where f, g are odd and coprime, but $|h| < |z|$. This conclusion points at an (impossible) *infinite descent*.

A weak point in the above argumentation is the claim of the existence of two integers s, t fulfilling (1). The missing steps can actually be recovered by means of some arithmetic properties of the integers of the form $a^2 + 3b^2$ presented by Euler in a memoir of 1760. A more elegant approach is based on the ring theory developed by Kummer and Dedekind in the following century. The main tool is the ring of integers of the number field $\mathbb{Q}(\omega)$, where ω is a primitive cubic root of unity. One can exploit the fact that it is a UFD.